Objet	**Déclaration des Pratiques de l'Opérateur de Dispositifs de Création de Signature à Distance 1.3.6.1.4.1.62714.51.1.33.1**

Version *	Date	Modifications	Rédacteur
0.1	04/09/2025	Création du document	GBA
1.0	03/03/2025	Première version complète	GBA

* *<Version>.<Edition>* *Changement de version = évolution majeure* *Changement d'édition = évolution mineure*

Durée de validité	*Nbre de versions à conserver*
1 an	Minimum 2 (actuelle + précédente)

Niveau de diffusion	*Liste de diffusion si Restreint ou Confidentiel*
Public	

	Fonction	Date & Signature
Vérificateur 1	DSSC GBA	*Signature manuscrite – version officielle conservée*
Vérificateur 2	Responsable d'AC SPA	*Signature manuscrite – version officielle conservée*
Approbateur	Administrateur Délégué LCA	*Signature manuscrite – version officielle conservée*

© Tous droits réservés be invest international SA - Toute reproduction ou diffusion même partielle interdite sans autorisation.

Sommaire

© Tous droits réservés be invest international SA - Toute reproduction ou diffusion même partielle interdite sans autorisation.

© Tous droits réservés be invest international SA - Toute reproduction ou diffusion même partielle interdite sans autorisation.

1 Introduction

1.1 Présentation générale

BE YS TRUSTED SOLUTIONS LUXEMBOURG, ci-après le Prestataire, s'est positionnée comme prestataire de services de confiance au service de ses clients et partenaires, offrant notamment un service d'opérateur de signature qualifiée à distance.

Le Prestataire a établi la présente Déclaration de Pratiques afin de décrire la manière dont il se conforme à la norme ETSI TS 119 431-1.

1.2 Objet du document

La présente Déclaration des Pratiques de l'Opérateur de Dispositifs de Création de Signature à Distance (DPC-ROQSCD) a pour objet de décrire l'ensemble des pratiques, procédures et mesures mises en œuvre par le Prestataire afin d'assurer la conformité de son service d'opérateur de signature qualifiée à distance aux exigences de la norme ETSI TS 119 431-1 – "Policy and Security Requirements for Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements", ainsi qu'aux prescriptions applicables du ETSI TS 119 431-2 relatives aux services d'opérateur.

Ce document établit le cadre organisationnel, opérationnel et de sécurité applicable au système de création de signature à distance exploité par le Prestataire.

Il définit notamment les principes relatifs à :

- la conception, la sécurité et le maintien en condition opérationnelle du système de signature à distance ;
- la gestion des composants critiques, incluant les dispositifs matériels de sécurité (HSM/QSCD), les modules logiciels et l'infrastructure de contrôle ;
- les processus de création de signature et d'authentification forte du signataire ;
- la gestion des identités, des credentials et des mécanismes d'activation des clés privées ;
- la gestion des risques, de la journalisation et des évènements de sécurité ;
- la continuité, la résilience et la surveillance du service d'opérateur.

La présente DPC-ROQSCD complète la Déclaration des Pratiques Générale (DPG) du Prestataire, à laquelle elle se réfère pour tous les aspects transverses de sécurité, d'organisation, de gouvernance, de gestion du personnel et de conformité, tels que définis dans la norme ETSI EN 319 401.

Elle précise les pratiques opérationnelles spécifiques au service de signature à distance, en conformité avec les normes ETSI 119 431-1 et 119 431-2 et, lorsque applicable, avec les exigences des QSCD qualifiés utilisés.

Cette DPC-ROQSCD s'inscrit dans le système de management de la sécurité et de la conformité du Prestataire, et s'articule avec :

- la Politique de Signature applicable au service ;
- les procédures internes d'exploitation, de surveillance et de sécurité ;
- les référentiels normatifs applicables, notamment ETSI TS 119 431-1 et ETSI EN 319 401.

L'objectif de cette DPC-ROQSCD est de démontrer que le Prestataire met en œuvre un ensemble cohérent et proportionné de mesures organisationnelles, techniques et procédurales garantissant :

- la confiance dans le système de signature à distance ;

© Tous droits réservés be invest international SA - Toute reproduction ou diffusion même partielle interdite sans autorisation.

- la maîtrise des risques associés aux opérations de création et d'activation des clés de signature ;
- la conformité aux exigences réglementaires eIDAS ;
- la continuité, la résilience et la sécurité du service d'opérateur de signature qualifiée à distance.

1.3 Périmètre d'application

La présente Déclaration des Pratiques de l'Opérateur de Dispositifs de Création de Signature à Distance (DPC-ROQSCD) s'applique à l'ensemble des activités, systèmes, composants, processus et personnels impliqués dans la fourniture du service d'opérateur de signature qualifiée à distance exploité par le Prestataire, tel que défini dans le règlement (UE) n°910/2014 (eIDAS) et les normes ETSI TS 119 431-1 et 119 431-2.

Elle s'applique dès lors que le service de signature à distance ou sa Politique de Signature fait explicitement référence à la présente DPC-ROQSCD.

Le périmètre couvre l'ensemble des exigences spécifiques à un système de création de signature à distance, et notamment :

- la conception, la mise en œuvre et le maintien en condition de sécurité du système de création et d'activation des clés de signature ;
- la gestion des dispositifs matériels et logiciels supports (dont QSCD/HSM) ;
- L'authentification forte du signataire et les mécanismes d'autorisation/activation de signature ;
- la gestion des identités, des credentials et des mécanismes cryptographiques associés ;
- la journalisation, la traçabilité, la détection et la gestion des incidents de sécurité ;
- la continuité opérationnelle, la résilience et la surveillance du service ;
- la gestion des interfaces de confiance avec les systèmes tiers ou complémentaires (ex. service d'identification, service de validation, services internes).

La présente DPC-ROQSCD s'inscrit dans le cadre général de sécurité, d'organisation et de conformité défini par la Déclaration des Pratiques Générale (DPG) du Prestataire, à laquelle elle se conforme et se réfère pour tous les aspects transverses, notamment :

- la gouvernance, l'organisation et les rôles de confiance ;
- la gestion de la sécurité physique, logique et opérationnelle ;
- la gestion des risques, de la continuité d'activité et des incidents ;
- la gestion du cycle de vie des clés et dispositifs cryptographiques ;
- la gestion des fournisseurs et sous-traitants ;
- le respect des exigences légales, réglementaires et normatives.

Les dispositions spécifiques au service de signature à distance sont détaillées dans la présente DPC-ROQSCD, tandis que la DPG fournit le socle commun de sécurité, d'organisation et de gouvernance applicable à l'ensemble des services de confiance du Prestataire.

1.4 Gestion du document

1.4.1 Procédure de mise à jour et de contrôle de version

© Tous droits réservés be invest international SA - Toute reproduction ou diffusion même partielle interdite sans autorisation.

Tout projet de modification du présent document doit rester conforme aux exigences de la politique de sécurité du Prestataire, de la norme [119431], de la [DPG] et respecter les engagements existants. En cas de changement important, l'AG de l'IGC du Prestataire pourra faire appel à une expertise technique pour en contrôler l'impact.

Le délai d'information est précisé dans la [DPG]

1.4.2 Publication et accessibilité (publique / restreinte)

Ce document de déclaration de pratique est un document public. Il est disponible sur le site de publication du Prestataire de service.

1.4.3 Périodicité des révisions

Le présent document devra faire l'objet d'une revue au moins une fois par an, pouvant entraîner ou non un amendement.

1.5 Responsables du maintien du document

Le Prestataire de service est responsable de ce document. Il s'assure périodiquement que le document est à jour, que son référentiel est correct. Il s'assure également de la cohérence entre ce document et la déclaration de pratique privée détaillant les procédures opérationnelles du service.

1.6 Références réglementaires et légales

Renvoi	Document
[DPG]	Déclaration de Pratiques Générale
[EIDAS]	Règlement européen eIDAS
[KM]	Procédure de Key Management

1.7 Références normatives

Renvoi	Document	Version
[319401]	ETSI EN 319 401 : Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers	3.1.1
[119431]	ETSI TS 119 431 : Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service providers;	1.3.1

1.8 Définitions, acronymes et abréviations

1.8.1 Définitions

Terme	Définition
Autorité de Gouvernance (AG) *[Governance Authority (GA)]*	Entité responsable de l'ensemble des fonctions de l'IGC avec pouvoir décisionnaire
Cérémonie des Clés ou Key Ceremony (KC)	Réunion spéciale des personnes autorisées pour générer le Certificat d'une AC ou d'un Client (KC Client). La Bi-clé de ce

© Tous droits réservés be invest international SA - Toute reproduction ou diffusion même partielle interdite sans autorisation.

	Certificat doit être générée avec toutes les précautions nécessaires (voir la DPC) pour éviter sa compromission
Chiffrement ***[Encryption]***	Transformation cryptographique d'un ensemble de données (clair) en vue de produire un ensemble chiffré (dit cryptogramme)
Client	Entité cliente ayant décidé de souscrire au Service du Prestataire, qu'elle utilise pour ses propres besoins ou qu'elle met à disposition des Utilisateurs.
Composante du Service de Confiance	Plate-forme opérée par une entité et constituée d'au moins un poste informatique, une application et, le cas échéant, un moyen de cryptologie et jouant un rôle déterminé dans la mise en œuvre opérationnelle d'au moins une fonction du Service de Confiance
Confidentialité ***[Confidentiality]***	Propriété d'une *information* ou d'une *ressource* de n'être accessible qu'aux utilisateurs autorisés (création, diffusion, sauvegarde, archivage, destruction)
Déchiffrement ***[Decryption]***	Transformation d'un cryptogramme en vue de retrouver les données originelles en clair
Déclaration des Pratiques de Certification (DPC) ***[Certification Pratice Statement (CPS)]***	Document qui identifie les pratiques (organisation, procédures opérationnelles, moyens techniques et humains) que l'AC applique dans le cadre de la fourniture de ses services de certification électronique aux usagers et en conformité avec la ou les PC qu'elle s'est engagée à respecter
Horodatage ***[Time-stamping]***	Service qui associe de manière sûre un événement et une heure afin d'établir de manière fiable l'heure à laquelle cet événement s'est réalisé
Infrastructure de Gestion de Clés (IGC) ***[Public Key Infrastructure (PKI)]***	Ensemble de composants, fonctions et procédures dédiées à la gestion de clés cryptographiques et de leurs Certificats utilisés par des services de confiance. Une IGC peut être composée d'une AC, d'un OC, d'une AE centralisée et/ou locale, de MC, d'une entité d'archivage, d'une entité de publication
Intégrité ***[Integrity]***	Propriété d'exactitude, de complétude et d'inaltérabilité dans le temps des *informations* et des *fonctions* de l'information traitée
Module cryptographique matériel ***[Hardware Cryptographic Module (HSM)]***	Matériel électronique offrant un service de sécurité qui consiste à générer, stocker et protéger des clés cryptographiques
Non-répudiation ***[Non-repudiation]***	Impossibilité pour un Porteur, un Utilisateur ou une Application utilisatrice de nier sa participation à un échange d'information ; cette participation porte tant sur l'origine de l'*information* (*imputabilité*) que sur son contenu (*intégrité*)
Politique de Certification (PC) ***[Certification Policy (CP)]***	Ensemble de règles, identifié par un nom (OID), définissant les exigences auxquelles une Autorité de Certification se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'un Certificat à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes. Une PC peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les Porteurs et les Applications utilisatrices de certificats
Produit de sécurité	Dispositif, de nature logicielle et/ou matérielle, dont l'utilisation est requise pour mettre en œuvre des fonctions

© Tous droits réservés be invest international SA - Toute reproduction ou diffusion même partielle interdite sans autorisation.

	de sécurité nécessaires à la sécurisation d'une information dématérialisée (lors d'un échange, d'un traitement et/ou du stockage de cette information). Ce terme générique couvre notamment les dispositifs de signature électronique, les dispositifs d'authentification et les dispositifs de protection de la confidentialité
Promoteur d'application	Fournisseur d'une offre de service sécurisé (échanges dématérialisés)
Service de Confiance	Service fournit par le Prestataire définit dans le règlement européen eIDAS [EIDAS]
Service du Prestataire	Un des services de la gamme d'offres de services de dématérialisation et de confiance du groupe du Prestaire, déployé en tout ou partie
Uniform Resource Locator (URL)	Adresse d'un site internet
Utilisateur	Voir « Application utilisatrice »

1.8.2 Acronymes et Abréviations

Acronyme FR	Acronyme EN	Définition
AC	**CA**	**Autorité de Certification [Certification Authority]**
AG	GA	Autorité de Gouvernance [Governance Authority]
CC	CC	Critères Communs [Common Criteria]
CEN		**Comité Européen de Normalisation**
CSP		Cryptographic Service Provider
DN		**Distinguished Name**
DPC	CPS	Déclaration des Pratiques de Certification [Certification Practice Statement]
EAL		**Evaluation Assurance Level**
ETSI		European Telecommunications Standards Institute
HSM		**Hardware Security Module**
KC		**Cérémonie des clés [Key Ceremony]**
OID		**Object Identifier**
PC	CP	Politique de Certification [Certification Policy]
PP	PP	Profil de Protection [Protection Profile]
RSA		Rivest Shamir Adelman
SSI		**Sécurité des Systèmes d'Information**
URL		Uniform Resource Locator

1.9 Identification du document

La présente déclaration de pratique est nommée « Déclaration des Pratiques de l'Opérateur de Dispositifs de Création de Signature à Distance».

Elle repose sur la norme « ETSI TS 119 431 : Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service providers;» [119431].

L'OID de ce document est 1.3.6.1.4.1.62714.51.1.33.1

Le préfixe d'OID de ce document répond aux principes de nommage suivant :

Iso(1).member-body(3).beystslu(6.1.4.1. 62714).remote-qscd(51).perimeter1(1).ps(33). version(1)

© Tous droits réservés be invest international SA - Toute reproduction ou diffusion même partielle interdite sans autorisation.

Le terme ps est utilisé pour Practice Statement, Déclaration de pratique en français.

2 Dispositions générales concernant la déclaration de pratiques et les politiques

2.1 Exigences relatives à la déclaration de pratiques

La présente Déclaration de pratiques est conforme aux exigences de la norme [319401]. Les dispositions transverses pertinentes sont définies dans la [DPG], à laquelle la présente Déclaration de Pratiques se réfère.

La publication de ce document suit les règles définies dans la [DPG].

2.2 Nom et identification de la Politique de service

La présente Déclaration de pratiques est conforme à la politique EU SSAS v2 (EUSPv2), telle que définie dans la norme ETSI TS 119 431-1. Cette politique s'applique à l'ensemble du périmètre couvert par la présente Déclaration de pratiques.

La politique de Service est la norme ETSI TS 119 431-01 en version 1.3.1.

2.3 Participants

2.3.1 Autorité de gouvernance

L'autorité de gouvernance est définie dans la [DPG]. Son fonctionnement et ses responsabilités dans le périmètre actuel est décrit dans cette [DPG].

2.3.2 Recours à des tiers

Le Prestataire peut s'appuyer sur des prestataires externes pour fournir certaines parties du service. Néanmoins, il demeure pleinement responsable de la conformité du service et de la mise en œuvre de toutes les exigences définies dans la présente Politique.

Le Prestataire s'assure que tout tiers impliqué respecte les exigences applicables.

Lorsque le tiers utilise un moyen d'identification électronique issu d'un schéma notifié au sens de l'article 9 du règlement (UE) n°910/2014, la conformité au niveau requis est réputée satisfaite.

2.3.3 Rôles et Habilitations

Les différents rôles et habilitations sont définis dans la procédure rôle et habilitation.

3 Gestion et exploitation du service

3.1 Publication et dépôt

La présente Déclaration de Pratiques ainsi que les informations associées sont publiées par le Prestataire via un dépôt électronique accessible publiquement.

La version en vigueur du document est disponible à l'adresse suivante :

http://pki.almerys.com

© Tous droits réservés be invest international SA - Toute reproduction ou diffusion même partielle interdite sans autorisation.

Le Prestataire garantit l'intégrité, la disponibilité et la traçabilité des documents publiés au moyen de mécanismes techniques et organisationnels appropriés, incluant la gestion des versions et le contrôle des accès administratifs.

Toute modification de la présente Déclaration de Pratiques est validée conformément aux procédures internes, puis publiée dans le dépôt officiel. Les versions précédentes sont conservées selon la politique de conservation définie dans la [DPG].

Les versions internes ou en cours d'élaboration sont stockées dans un référentiel documentaire sécurisé, accessible uniquement aux personnes autorisées.

3.2 Initialisation de la clé de signature

Le document Key management [KM] apporte des détails complémentaires sur cette partie.

3.2.1 Génération de la clé de signature

Avant toute utilisation, le dispositif cryptographique sécurisé (SCDev) est initialisé au moyen de mécanismes techniques imposant l'intervention d'au moins deux opérateurs.

Cette initialisation repose sur les fonctions de contrôle d'accès et de séparation des rôles du SCDev (mécanismes de quorum), garantissant qu'aucun opérateur ne peut seul initialiser, activer ou configurer le dispositif.

L'initialisation du SCDev est réalisée conformément aux procédures d'exploitation du Prestataire et aux exigences de sécurité de la présente Déclaration de pratiques.

Les clés privées sont générées et utilisées exclusivement au sein d'un dispositif cryptographique sécurisé (SCDev). Le Prestataire utilise des modules matériels de sécurité évalués conformément aux Critères Communs EAL4+ avec renforcement AVA_VAN.5, répondant ainsi aux exigences de la politique [119431].

Le SCDev répond aux mécanismes de sécurité requis pour la génération, la protection et l'utilisation des clés privées dans le cadre des opérations du SSAS.

Aucune clé privée ne quitte le dispositif ni n'est accessible hors de l'environnement protégé du SCDev.

3.2.2 Moyens d'identification électronique ou mécanismes de liaison d'identité

L'authentification du signataire repose sur un moyen d'identification électronique fourni par un fournisseur d'identité externe (IdP).

Le processus d'enrôlement est réalisé par le même Prestataire de Services de Confiance que l'Autorité de Certification, via son Autorité d'Enregistrement ou une Autorité d'Enregistrement déléguée, conformément aux exigences d'enrôlement définies dans EN 419241-1.

L'identification et la vérification d'identité sont réalisées avec un niveau d'assurance au moins substantial, notamment au moyen d'un processus d'identification à distance avec preuve vidéo (PVID) ou lors d'un face à face physique.

Ces exigences s'appliquent :

- aux personnes physiques, conformément aux exigences applicables d'identification substantielle ;
- aux personnes morales, via la vérification du représentant et des attributs d'organisation selon les procédures d'enregistrement du Prestataire.

© Tous droits réservés be invest international SA - Toute reproduction ou diffusion même partielle interdite sans autorisation.

L'authentification du signataire est effectuée par la solution d'identité Belam, opérée par une entité du groupe en dehors du périmètre opérationnel du SSASP.

Le Prestataire s'assure contractuellement et techniquement que ce fournisseur d'identité respecte les exigences applicables en matière d'identification, d'authentification et de sécurité.

La liaison entre l'identité du signataire, la référence du moyen d'identification électronique et la clé de signature est réalisée au niveau applicatif par la plateforme de signature Signer6, qui assure le binding entre l'identité validée et le certificat associé.

Le Prestataire garantit que les données d'identification utilisées lors de l'authentification sont cohérentes avec celles présentes dans le certificat du signataire.

L'intégrité du lien entre la clé de signature et la référence du moyen d'identification électronique est protégée par les mécanismes de sécurité du système de signature et par les contrôles d'accès associés.

3.2.3 Association avec le certificat

Lors du processus d'initialisation, le composant de signature associe systématiquement chaque clé de signature du signataire avec le certificat de clé publique correspondant. Cette liaison clé–certificat est réalisée avant toute utilisation opérationnelle de la clé.

Ce composant est configuré pour interdire toute opération de signature tant que la clé privée du signataire n'est pas liée à son certificat de clé publique, conformément aux exigences de la présente Politique.

L'intégrité de la liaison entre la clé de signature et le certificat est assurée par le Module d'accès sécurisé (Security Access Module - SAM), qui protège les références associées et empêche toute modification non autorisée.

3.3 Gestion du cycle de vie de clés de signature

3.3.1 Activation de la signature

L'activation d'une clé de signature par le Signer SAM est strictement conditionnée par la réception de données d'activation de signature (SAD) valides, incluant un jeton d'autorisation attestant de l'authentification réussie du signataire. Le Signer SAM vérifie la validité, l'intégrité et le contexte d'utilisation de ces SAD avant toute activation de la clé.

Les mécanismes d'échange et de transport des SAD assurent la confidentialité et l'intégrité des données et protègent contre les attaques de type interception, rejeu, substitution ou élévation de privilèges. Les SAD sont liées au contexte de signature et ne peuvent être réutilisées en dehors de celui-ci.

Le modèle de contrôle d'accès appliqué au SASS repose sur le principe du moindre privilège. Le signataire ne peut accéder qu'aux fonctions nécessaires à l'initiation de ses opérations de signature, sans possibilité d'interagir avec des objets critiques du système ni d'influencer les clés ou opérations d'autres utilisateurs.

Le SASS garantit que toute opération de signature est réalisée exclusivement avec la clé de signature associée au signataire authentifié. Le Signer SAM n'active la clé que lorsque les SAD démontrent une authentification valide et un lien correct avec l'identité du signataire.

Une fois activée, la clé de signature est utilisée uniquement pour signer les données explicitement autorisées par la Plateforme de Signature. L'application de signature assure la collecte du consentement du signataire et vérifie que chaque opération de signature correspond à une intention explicite et valide.

© Tous droits réservés be invest international SA - Toute reproduction ou diffusion même partielle interdite sans autorisation.

3.3.2 Suppression de la clé de signature

Le Prestataire met en œuvre des procédures garantissant que toute clé de signature est détruite dès qu'elle n'est plus utilisable, notamment lorsque le certificat public associé est expiré ou lorsque la clé est devenue inutile pour le signataire (expiration, révocation définitive). Lorsque le lien entre la clé et le signataire n'est pas maintenu après une session de signature, la clé est automatiquement détruite à la fin de ladite session, sans possibilité de réinsertion, de récupération ou de réutilisation ultérieure.

La destruction est réalisée dans le module cryptographique, selon les mécanismes sécurisés prévus, ou par la destruction des clés wrapped lorsqu'elles existent. Ce processus entraîne l'impossibilité totale de restaurer la clé. Il est déclenché automatiquement, sans intervention manuelle, et fait l'objet d'une journalisation complète.

Le Prestataire s'assure que toutes les occurrences actives de la clé dans le module cryptographique sont irréversiblement effacées, et qu'aucune information résiduelle ne permettrait d'en reconstituer les éléments.

S'agissant des sauvegardes, les clés ne sont jamais conservées en clair (voir section 3.3.3). Lorsqu'une clé est présente sous forme de wrapped key dans une base de données, elle demeure protégée par des mécanismes cryptographiques garantissant son inutilisabilité hors du module cryptographique. Conformément aux limitations techniques admises, la suppression ciblée d'une clé individuelle dans une sauvegarde n'est pas réalisable. Toutefois, la politique de sauvegarde prévoit une durée de rétention maîtrisée, assurant que toute sauvegarde contenant une version protégée d'une clé détruite est automatiquement supprimée à l'issue de cette période.

Ainsi, le dispositif garantit que la clé opérationnelle est immédiatement détruite dans l'environnement actif et que toutes les sauvegardes qui pourraient en contenir une version protégée sont éliminées dans un délai contrôlé, empêchant toute possibilité de récupération future.

3.3.3 Sauvegarde et restauration de la clé de signature

Le Prestataire garantit que toutes les clés privées ou secrètes, y compris les clés de signature du signataire, les clés d'infrastructure et les clés de contrôle, sont stockées exclusivement dans un environnement sécurisé.

Les clés ne sont jamais stockées en clair ou sous une forme non protégée. Elles sont générées, manipulées et stockées dans des modules cryptographiques offrant un niveau de protection conforme aux exigences de sécurité du système.

Les clés sont stockées protégées par un chiffrement uniquement connu du matériel cryptographique. Le nombre de sauvegarde (id est le nombre de back up de la base) n'excède pas le nombre nécessaire de copie nécessaire pour assurer la continuité de service.

Dans les rares cas où une clé privée ou secrète doit être exportée hors du module sécurisé, le Prestataire s'assure que :

- l'export est réalisé uniquement sous forme protégée, garantissant confidentialité et intégrité ;
- le niveau de protection appliqué est au moins équivalent à celui garanti à l'intérieur du module cryptographique ;
- lorsqu'une clé est protégée par chiffrement, seuls des algorithmes cryptographiques et paramètres conformes aux exigences de robustesse actuelles sont utilisés ;
- toute opération d'export nécessite des autorisations spécifiques et est enregistrée dans les journaux de sécurité.

© Tous droits réservés be invest international SA - Toute reproduction ou diffusion même partielle interdite sans autorisation.

Aucun export de clé privée du signataire ou d'une clé critique n'est autorisé sans justification opérationnelle, contrôle préalable et sécurisation conforme aux politiques internes.

Le Prestataire a mis en place des procédures garantissant que :

- Les opérations de sauvegarde, stockage ou restauration des clés privées ou secrètes (clés de signature, clés d'infrastructure, clés de contrôle) sont effectuées exclusivement par du personnel autorisé, spécifiquement formé et désigné.
- Les master keys utilisées pour protéger les clés utilisateurs et les clés de travail :
  - sont manipulées sous contrôle multiple (dual control) ;
  - ne sont jamais détenues en clair hors du module cryptographique ;
  - sont stockées et sauvegardées dans un format protégé, garantissant leur confidentialité et intégrité.
- Toute opération impliquant une master key fait l'objet :
  - d'un contrôle d'accès renforcé,
  - d'une traçabilité complète dans les journaux du système,
  - d'une supervision par les rôles autorisés définis dans la politique de sécurité.

Ces mesures garantissent que les clés critiques ne peuvent être compromises lors de leur gestion, et que les exigences de sécurité du SASS sont systématiquement respectées.

3.4 Installations, gestion et contrôles opérationnels

3.4.1 Général

L'ensemble de la section 4.4 de la [DPG] s'applique.

3.4.2 Mesure de sécurité physique

L'ensemble de la section 4.8 de la [DPG] s'applique.

En particulier :

Le Prestataire opère les installations dédiées à la génération et à la gestion de révocation des certificats dans des environnements physiquement sécurisés, protégeant les systèmes et les données contre toute tentative d'accès non autorisé.

Une périmétrie de sécurité est clairement définie par utilisation de matériel dédié dans des baies dédiées à l'usage du Prestataire.

L'accès à la zone sécurisée est strictement contrôlé :

- Chaque entrée et sortie est enregistrée dans un journal dédié ;
- Tout accès est soumis à une supervision indépendante ;
- Les personnes non autorisées ne peuvent pénétrer dans la zone que si elles sont constamment accompagnées par un personnel autorisé ;
- Seul le personnel explicitement autorisé peut intervenir dans cette zone, y compris pour les fonctions additionnelles du TSP qui y seraient éventuellement hébergées.

Le Prestataire met en œuvre des mesures de sécurité physique et environnementale visant à protéger les locaux, les ressources critiques et les infrastructures de support, notamment vis-à-vis :

© Tous droits réservés be invest international SA - Toute reproduction ou diffusion même partielle interdite sans autorisation.

- des accès physiques non autorisés ;
- des catastrophes naturelles ;
- des incendies ;
- des défaillances de services essentiels (énergie, climatisation, télécommunications) ;
- des risques structurels (effondrement, fuites d'eau) ;
- du vol, de l'effraction ou de la perte de disponibilité.

Des contrôles renforcés garantissent qu'aucun équipement, information, support ou logiciel lié aux services du Prestataire ne peut être retiré du site sans autorisation préalable.

L'ensemble de ces mesures est formalisé dans la politique de sécurité physique et environnementale du Prestataire et appliqué de manière cohérente sur tous les sites concernés par la génération et la gestion de révocation des certificats.

3.4.3 Mesures organisationnelles procédurales

L'ensemble de la section 4.5 de la [DPG] s'applique.

3.4.4 Mesures de sécurité liées au personnel

L'ensemble de la section 4.3 de la [DPG] s'applique.

3.4.5 Procédures de journalisation d'audit.

Le Prestataire enregistre et conserve, pendant une durée appropriée y compris après une éventuelle cessation d'activité, l'ensemble des informations pertinentes émises ou reçues dans le cadre de l'exploitation des services de confiance. Ces informations sont conservées notamment afin de fournir des preuves en cas de procédure légale et d'assurer la continuité du service.

3.4.5.1 Confidentialité, intégrité et archivage des enregistrements

Le Prestataire met en œuvre des mesures techniques et organisationnelles garantissant la confidentialité, l'intégrité et la protection des enregistrements relatifs au fonctionnement des services, qu'ils soient actifs ou archivés. Ces enregistrements comprennent notamment :

- les journaux d'audit,
- les traces d'exploitation et d'accès,
- les événements de sécurité,
- les opérations de gestion des clés,
- les événements environnementaux et systèmes critiques,
- toute information pertinente pour démontrer la conformité du service.

L'archivage est réalisé conformément aux pratiques opérationnelles publiées dans la Politique de Certification, la Déclaration de Pratiques de Certification, les politiques de sécurité ainsi que les Conditions Générales.

Les accès aux archives sont strictement limités au personnel autorisé.

Les enregistrements pertinents sont mis à disposition lorsqu'ils sont nécessaires pour démontrer le bon fonctionnement des services, notamment dans le cadre de procédures judiciaires ou de contrôles réglementaires.

La traçabilité est assurée par l'enregistrement systématique des événements dans des tickets permettant de documenter décisions, actions et résultats.

© Tous droits réservés be invest international SA - Toute reproduction ou diffusion même partielle interdite sans autorisation.

Le Prestataire enregistre avec précision l'heure de tous les événements significatifs liés :

- à l'environnement physique (alarmes, incidents, pannes d'infrastructure),
- à la gestion du cycle de vie des clés cryptographiques (génération, usage, rotation, destruction),
- à la synchronisation temporelle et aux anomalies associées.

Les horodatages utilisent une source de temps fiable, synchronisée plusieurs fois par jour avec UTC, garantissant cohérence, exactitude et valeur probante.

Les enregistrements sont conservés pendant une durée de sept ans plus l'année en cours, conformément aux Conditions Générales, afin d'assurer la disponibilité des preuves nécessaires.

Les journaux sont centralisés, protégés contre la modification ou la suppression non autorisée par des mécanismes cryptographiques (chaînage, signature, append-only).

La suppression n'est autorisée qu'après archivage fiable sur un support longue durée.

Tous les événements de sécurité significatifs sont journalisés, incluant :

- les modifications de configuration ou de politique de sécurité,
- les démarrages, arrêts et redémarrages (y compris après crash),
- les défaillances matérielles,
- l'activité des pare-feux et routeurs,
- les tentatives d'accès aux systèmes du SSAS/TW4S.

Un historique des changements de configuration système, applicatif et réseau est conservé.

Tous les accès, y compris tentatives, sont journalisés.

3.4.5.2 Conformité aux exigences d'audit de la norme [419241]

Le Prestataire a choisi une solution logicielle de signature intégrant nativement l'ensemble des mécanismes nécessaires pour satisfaire les exigences d'audit définies dans les sections SRG_AA de [419241]. Cette solution permet notamment la journalisation complète des événements pertinents, la gestion correcte de leur transfert vers des stockages externes, la conservation de toutes les données d'audit, ainsi que la mise en œuvre des mécanismes de protection et d'intégrité attendus.

La solution garantit que les journaux ne peuvent être ni supprimés ni altérés avant leur export, et qu'ils ne peuvent être enrichis que par ajout, grâce à des mécanismes cryptographiques de chaînage et de protection en écriture. L'ensemble des données d'audit est archivé de manière sécurisée afin d'éviter toute perte.

Les enregistrements produits contiennent systématiquement les informations requises (horodatage précis, type d'événement, identité de l'entité responsable, succès ou échec), et leur intégrité peut être vérifiée via les fonctionnalités prévues par le logiciel.

En complément, l'horodatage des événements repose sur l'horloge sécurisée du module cryptographique, synchronisée conformément aux exigences applicables, garantissant ainsi l'exactitude et la cohérence temporelle de toutes les traces.

3.4.6 Archivage des enregistrements

Le Prestataire conserve l'ensemble des données d'audit pendant une durée minimale de sept ans, plus l'année en cours, après l'expiration de tout certificat auquel ces enregistrements se rapportent, conformément aux exigences applicables et dans le respect de la législation en vigueur.

© Tous droits réservés be invest international SA - Toute reproduction ou diffusion même partielle interdite sans autorisation.

Les données d'audit sont archivées dans les centres de données internes du Prestataire, et une copie supplémentaire est conservée dans un centre de données distant opéré par un prestataire externe, garantissant une redondance géographique et la disponibilité des informations archivées.

3.4.7 Gestion des compromissions et reprise après sinistre

3.4.7.1 Gestion des vulnérabilités et des incidents

3.4.7.1.1 Surveillance et journalisation

Le Prestataire met en place des mécanismes de surveillance continue permettant de détecter tout incident de sécurité potentiel, grâce à des outils et processus assurant la collecte, la journalisation et l'analyse des événements issus des réseaux et systèmes d'information. Une procédure de traitement des incidents de sécurité formalise les actions à mener.

La surveillance tient compte de la sensibilité des informations collectées, en limitant leur volume aux seuls éléments nécessaires, en protégeant les journaux susceptibles de contenir des données sensibles et en respectant les règles de confidentialité applicables.

Le Prestataire détecte et signale sous forme d'alertes toute activité anormale susceptible d'indiquer une violation de sécurité, notamment via des scans réguliers, des tests d'intrusion annuels et la présence d'un SOC/SIEM capable d'identifier et de notifier les comportements suspects.

Le Prestataire tient à jour et révise régulièrement des journaux couvrant au minimum :

- le trafic réseau entrant et sortant ;
- les actions d'administration, de gestion des droits et les accès, notamment privilégiés ;
- les actions effectuées avec des comptes administrateur ;
- les accès et modifications aux fichiers critiques et sauvegardes ;
- les journaux de sécurité pertinents ;
- l'usage et la performance des ressources système ;
- les accès physiques lorsque pertinent ;
- l'accès et l'usage des équipements réseau ;
- les événements environnementaux lorsque applicable.

Les systèmes sont soumis à une surveillance régulière, incluant l'examen automatisé des journaux d'audit et l'alerte du personnel en cas d'événements critiques. Une revue manuelle complémentaire est également effectuée.

3.4.7.1.2 Réponse aux incidents

Le Prestataire applique une procédure de traitement des incidents, couvrant les phases de confinement, d'éradication et de restauration du service. Cette procédure décrit également les obligations de notification prévues par les cadres législatifs applicables (eIDAS, NIS/DORA, règlement sectoriel), conformément à la Déclaration de Pratiques Générale [DPG].

La communication vers les parties prenantes suit les plans de communication définis dans la [DPG], incluant la classification des incidents, les processus d'escalade et les protocoles de notification.

Le Prestataire garantit que le personnel dispose des compétences nécessaires pour détecter et gérer efficacement les incidents de sécurité. Chaque incident fait l'objet d'un ticket assurant la traçabilité complète des actions, décisions et résultats.

© Tous droits réservés be invest international SA - Toute reproduction ou diffusion même partielle interdite sans autorisation.

Les rôles, responsabilités et procédures sont testés et revus régulièrement, notamment dans une logique d'amélioration continue. Les réunions trimestrielles de revue d'incidents permettent d'ajuster les pratiques et de suivre l'application des actions correctives.

Les vulnérabilités critiques sont traitées dans un délai maximal de 48 heures à compter de leur découverte. Pour toute autre vulnérabilité, le Prestataire établit un plan de mitigation ou documente, dans la procédure dédiée, la justification de l'absence de correction lorsqu'elle est dûment argumentée.

Les procédures de réponse sont mises en œuvre de manière à minimiser l'impact des incidents. Le suivi des alertes critiques est confié à du personnel habilité, conformément à la procédure de traitement des incidents.

3.4.7.1.3 Notification et communication des incidents

Le Prestataire applique une procédure de notification permettant d'informer les parties appropriées de toute violation de sécurité ou perte d'intégrité ayant un impact significatif, dans un délai maximal de 24 heures après identification, conformément aux obligations réglementaires.

Lorsque l'incident est susceptible d'affecter une personne physique ou morale utilisatrice du service, celle-ci est notifiée sans délai injustifié.

Le Prestataire maintient une procédure simple permettant à son personnel, à ses sous-traitants et à ses clients de signaler tout incident potentiel, et communique cette procédure aux parties concernées. Le personnel reçoit une formation pour appliquer correctement cette procédure et contacter les interlocuteurs appropriés.

3.4.7.1.4 Évaluation, Revue et classification des événements

Le Prestataire analyse les événements signalés afin d'en évaluer la sévérité, de suivre l'évolution de l'incident et d'adapter la classification en fonction de nouvelles informations. La gestion par ticket d'incident documente les décisions, les corrections apportées ainsi que les analyses post-incident et les éventuelles mesures supplémentaires nécessaires.

Le Prestataire se tient informé des vulnérabilités techniques affectant ses systèmes grâce à des sources d'information dédiées et à des scans de vulnérabilité réguliers. L'exposition du Prestataire aux vulnérabilités identifiées est évaluée et des mesures adaptées sont mises en œuvre.

Pour chaque incident, le Prestataire conduit une revue post-incident, incluant l'identification de la cause racine et la mise en place d'actions destinées à réduire le risque de récurrence. Toutes les revues post-incident sont systématiquement réalisées et intégrées au processus d'amélioration continue.

3.4.7.2 Gestion de la continuité d'activité

Le Prestataire dispose d'un plan de continuité d'activité formalisé et maintenu à jour, décrit dans un document spécifique, permettant d'assurer la poursuite ou la reprise des services en cas de sinistre, y compris en situation de compromission d'une clé de signature privée ou de tout autre élément d'authentification du Prestataire.

En cas de sinistre, les opérations sont rétablies dans un délai maximal de quatre heures, conformément aux dispositions du plan de continuité. Ce plan prévoit notamment la mise en œuvre de solutions de contournement ainsi que les délais pour l'application des mesures correctives destinées à éliminer les causes susceptibles de provoquer une récurrence du sinistre.

Le Prestataire maintient des sauvegardes régulières et dispose de ressources suffisantes (infrastructures, réseaux, systèmes d'information, personnel) conformément aux résultats de l'évaluation de risques et au plan de continuité :

© Tous droits réservés be invest international SA - Toute reproduction ou diffusion même partielle interdite sans autorisation.

- Serveurs et bases de données : des sauvegardes sont effectuées régulièrement et transférées en continu vers le site secondaire.
- Modules cryptographique : tout élément généré sur le site principal est transmis vers le site secondaire après sa création.

Les plans de sauvegarde définissent notamment :

- les temps de reprise visés ;
- l'assurance de la complétude et de l'exactitude des sauvegardes;
- le stockage des sauvegardes dans un emplacement sécurisé, physiquement séparé du site principal et hors du réseau de production ;
- les mesures de protection physiques, environnementales et logiques adaptées à la classification de l'information ;
- les procédures de restauration, incluant les autorisations nécessaires.

Le Prestataire réalise des contrôles d'intégrité sur les sauvegardes, garantissant l'absence de corruption, et exécute des tests périodiques de restauration, notamment dans le cadre des exercices du plan de reprise d'activité. Les résultats de ces tests sont documentés, et des actions correctives sont mises en œuvre si nécessaire.

Le Prestataire a établi une procédure de gestion de crise, décrite dans un document dédié, définissant :

- les rôles et responsabilités en situation de crise ;
- les communications obligatoires ou volontaires avec les autorités compétentes ;
- les mesures visant à maintenir la sécurité des réseaux et des systèmes d'information pendant la crise.

Le Prestataire applique également un processus de traitement des informations reçues du CSIRT national ou, le cas échéant, d'autres autorités compétentes, processus assuré par le Trust Center.

Le plan de gestion de crise est testé annuellement et revu à intervalles planifiés ou à l'issue de tout incident majeur, afin d'assurer son efficacité opérationnelle.

3.4.8 Cessation du service

Le Prestataire dispose d'un plan de cessation d'activité à jour, documenté dans un référentiel dédié, garantissant que toute interruption définitive de ses services entraîne un impact mesuré sur les abonnés, les parties de confiance et les autres entités dépendantes. Ce plan assure notamment la préservation et la disponibilité des informations nécessaires à la vérification des services de confiance pendant une période appropriée.

Avant toute cessation de service, le Prestataire applique les mesures suivantes :

- Notification des parties concernées : le Prestataire informe l'ensemble des abonnés, des parties de confiance, des prestataires avec lesquels il entretient des relations contractuelles ou opérationnelles, ainsi que les autorités compétentes. Les informations relatives à la cessation sont également mises à disposition des autres parties de confiance n'ayant pas de relation directe avec le Prestataire.
- Fin des autorisations des sous-traitants : toutes les autorisations accordées aux sous-traitants pour agir au nom du Prestataire dans le cadre de services de confiance sont révoquées avant la cessation.
- Transfert ou maintien des obligations : le Prestataire organise, lorsque cela est possible, la transmission des services existants vers un autre Prestataire de Services de Confiance afin de garantir la continuité pour les clients concernés. Le Prestataire transfère également à une entité fiable les obligations liées à la conservation des informations nécessaires pour démontrer l'opération des services de confiance

© Tous droits réservés be invest international SA - Toute reproduction ou diffusion même partielle interdite sans autorisation.

pendant une durée raisonnable, à moins qu'il ne soit démontré qu'il ne détient aucune information relevant de cette obligation.

- Destruction sécurisée des clés privées : les clés privées du Prestataire, y compris leurs copies de sauvegarde, sont détruites ou retirées d'usage de manière à empêcher toute récupération.

Le Prestataire a également mis en place un dispositif financier permettant de couvrir les coûts associés à l'exécution de ces obligations en cas de faillite ou d'impossibilité de les assumer lui-même, dans la limite de la législation applicable.

Enfin, le Prestataire garantit que ses clés publiques, ainsi que les informations nécessaires à la validation des éléments de confiance, demeurent accessibles aux parties de confiance pendant une période raisonnable, directement ou par l'intermédiaire d'une entité fiable.

3.5 Mesures de sécurité technique

3.5.1 Gestion des rôles

La gestion des rôles définie dans la [DPG].

3.5.2 Opérations

Le Prestataire opérant le service SASS met en œuvre toutes les mesures nécessaires pour garantir que les fonctions de gestion opérationnelle du système sont protégées de manière adéquate et conformes aux recommandations du fabricant.

Le Prestataire s'assure notamment que :

- Le SASS est correctement et en toute sécurité opéré, conformément aux instructions officielles du fabricant. À cet effet, seules les procédures validées et documentées sont appliquées par le personnel autorisé.
- Le SASS est déployé de manière à minimiser les risques de défaillance du système. Les mesures suivantes sont systématiquement mises en place :
    - Redondance et séparation des composants critiques ;
    - Surveillance continue de l'état du système ;
    - Procédures de bascule et de reprise validées ;
    - Contrôles réguliers d'intégrité et de conformité.
- Le SASS est protégé contre les virus et logiciels malveillants, afin de garantir l'intégrité du système et des informations traitées. Cela inclut :
    - L'utilisation de solutions anti-malware ;
    - La mise en place de mécanismes de contrôle d'accès stricts ;
    - L'application régulière de correctifs de sécurité ;
    - La réalisation périodique de scans d'intégrité et d'audits de sécurité.

Le Prestataire veille à ce que toutes ces mesures soient continuellement maintenues, évaluées et améliorées dans le cadre du système de management de la sécurité.

Un Centre Opérationnel de Sécurité (SOC) est en place et assure une surveillance continue de la plateforme afin de détecter, analyser et signaler tout événement anormal ou suspect pouvant affecter la sécurité ou la disponibilité des services.

3.5.3 Mesures de sécurité

© Tous droits réservés be invest international SA - Toute reproduction ou diffusion même partielle interdite sans autorisation.

Les mesures indiquées au chapitre 4.5 de la [DPG] sont appliqués.

3.5.4 Mesures de sécurité appliquées au cycle de vie

Les mesures appliquées à la sécurité des opérations sont définies dans le chapitre 4.8 de la [DPG].

Les mesures appliquées à la gestion des Fournisseurs sont définies dans le chapitre 4.15 de la [DPG].

3.5.5 Mesures de sécurité des réseaux

Les mesures appliquées à la sécurité des réseaux sont définies dans le chapitre 4.9 de la [DPG].

3.6 Autres aspects commerciaux et juridiques

3.6.1 Tarifs

Le Prestataire se réserve le droit de facturer ses services conformément à ses conditions générales.

Les informations suivantes sont fournies dans les différents documents contractuels établis entre les parties : (i.e. Prestataire, les Clients du service, et éventuellement les fournisseurs assurant en tout ou partie certaines fonctions du Service) :

- Les conditions de facturation du Service proposé par le Prestataire ;
- Les responsabilités ;
- Les responsabilités financières ;
- Le montant des indemnités.

3.6.2 Responsabilité financière

La responsabilité financière du Prestataire est traitée à la section 3.6.1

3.6.3 Protection des données à caractère personnel

Le Prestataire applique les exigences de protection des données personnelles définies dans l'ETSI EN 319 401, notamment le REQ 7.13-05, et met en œuvre les mesures techniques et organisationnelles nécessaires pour assurer la confidentialité, l'intégrité et la conformité réglementaire du traitement de ces données.

3.6.4 Droits de propriété intellectuelle

Tous les droits de propriété intellectuelle détenus par le Prestataire sont protégés par la loi, règlement et autres conventions internationales applicables. Ils sont susceptibles d'entraîner la responsabilité civile et pénale en cas de non-respect.

La contrefaçon de marques de fabrique, de commerce et de services, dessins et modèles, signes distinctif, droits d'auteur (par exemple : logiciels, pages web, bases de données, textes originaux, …) est sanctionnée conformément aux dispositions des lois Luxembourgeoises.

3.6.5 Déclarations et garanties

Les déclarations et garanties applicables sont définies à la section 6.5.4, conformément à OVR-6.5.4-01.

Le PSC demeure responsable du respect des procédures prescrites par la présente politique, y compris lorsque certaines de ses fonctionnalités sont confiées à des prestataires externes.

3.6.6 Limitations de responsabilité

© Tous droits réservés be invest international SA - Toute reproduction ou diffusion même partielle interdite sans autorisation.

Sous réserve des dispositions d'ordre public applicables, Le Prestataire ne pourra pas être tenue responsable d'une utilisation non autorisée ou non conforme du service, des données d'activation ainsi que de tout autre équipement ou logiciel mis à disposition.

Le Prestataire décline en particulier sa responsabilité pour tout dommage résultant :

- D'un emploi du service pour un usage autre que ceux prévus avec le Client ;
- De l'usage de Certificats expirés ;
- D'un cas de force majeure (cad pour tout dommage dû à une cause indépendante de sa volonté, y compris, mais sans s'y limiter émeutes, pillages, sabotages, attaques ou actions criminelles; les dommages causés par des événements accidentels et incontrôlables, attribuables à des tiers (y compris, sans limitation, les incendies, les explosions, les accidents d'avion); catastrophes naturelles; les phénomènes atmosphériques (y compris, sans limitation, les inondations, les pluies, les vents, les tempêtes, les incendies, les ouragans, l'activité volcanique); l'échec des fournisseurs tiers à effectuer; conflits de travail ou actes gouvernementaux).

3.6.7 Indemnités

Se référer au chapitre 3.6.1

3.6.8 Amendements

Tout projet de modification de la présente Déclaration de Pratiques doit rester conforme aux exigences de la politique de sécurité du Prestataire, de la Politique identifiée dans ce document et respecter les engagements avec les Clients existants. En cas de changement important, l'AG du Prestataire pourra faire appel à une expertise technique pour en contrôler l'impact.

La procédure d'amendement intègre l'information et les délais d'information concernant les amendements.

La présente Déclaration de Pratiques devra faire l'objet d'une revue au moins une fois par an, pouvant entraîner ou non un amendement.

3.6.9 Procédures de règlement des litiges

Pour toute demande d'information ou réclamation relative au service du Prestataire, il convient de contacter le service Autorité de Certification par mail à l'adresse suivante : gouvernance.igc@be-ys.com.

En cas de litige sur l'interprétation du contenu ou l'exécution de la présente PC, une résolution amiable des conflits est privilégiée.

3.6.10 Droit applicable

Le droit applicable à tout litige relatif à l'interprétation et l'exécution de la présente Déclaration de Pratique est le droit du Luxembourg.

3.6.11 Conformité à la législation applicable

Le Prestataire se conforme à la législation et aux réglementations en vigueur et conserve les éléments de preuve de cette conformité. En particulier, chaque fois que cela est possible, le Prestataire :

- Met en place des moyens pour faciliter l'accès de ses services aux personnes en situation de handicap ;
- Traite les données personnelles en conformité avec la Réglementation en vigueur.

© Tous droits réservés be invest international SA - Toute reproduction ou diffusion même partielle interdite sans autorisation.

3.7 Autres dispositions

Le chapitre 4.14 de la [DPG] sur la conformité s'applique.

4 Algorithmes cryptographiques et paramètres de sécurité

La présente Déclaration de pratiques décrit l'ensemble des algorithmes et paramètres cryptographiques utilisés dans le cadre du Service de Signature Serveur. Ces algorithmes sont sélectionnés conformément à la norme ETSI TS 119 431-1, aux exigences eIDAS ainsi qu'aux recommandations européennes actuelles en matière de robustesse cryptographique.

Les paramètres cryptographiques utilisés pour la création de signature au sein du système de confiance sont sélectionnés de manière à garantir une résistance conforme à la durée de vie du certificat du signataire, assurant ainsi un niveau de sécurité approprié pendant toute leur période d'usage.

4.1 Algorithmes et paramètres de signature

Les signatures électroniques sont générées au moyen des algorithmes suivants :

- RSA 3072 bits, utilisant :
  - Schéma de signature RSASSA-PSS ;
  - Fonction de hachage SHA-256 ou supérieure ;
  - Paramètres PSS par défaut conformes à FIPS 186-5 (saltLength = 32, maskGen = MGF1-SHA-256).
- Elliptic Curve (EC) :
  - ECDSA avec courbe P-256, hachage SHA-256 ;
  - (Optionnel selon implémentation) ECDSA P-384 avec SHA-384.

Les profils de signature respectent ETSI EN 319 412 et ETSI EN 319 122 lorsqu'applicable.

4.2 Algorithmes de génération de paires de clés

Les paires de clés utilisées pour les opérations de signature sont générées exclusivement au sein du QSCD/HSM du Prestataire, conformément aux exigences eIDAS.

Les algorithmes et paramètres utilisés sont :

- RSA 3072 bits (génération interne HSM) ;
- ECDSA / P-256 (ou P-384 si activé).

La génération utilise l'implémentation conforme FIPS 140-2/140-3 du module cryptographique présent dans le dispositif certifié.

4.3 Autres algorithmes et paramètres critiques

Fonctions de hachage suivantes sont utilisées :

- SHA-256 (par défaut)
- SHA-384 (si nécessaire pour des profils EC)
- SHA-512 (si requis par un usage particulier)

Algorithmes de chiffrement (si nécessaires) :

© Tous droits réservés be invest international SA - Toute reproduction ou diffusion même partielle interdite sans autorisation.

- AES-256 en mode GCM (chiffrement des données internes, state protection, clés d'activation…)

Mécanismes d'intégrité et d'authentification :

- HMAC-SHA-256
- HMAC-SHA-384 (selon configuration interne)

La génération des paires de clés est effectuée au sein du QSCD/HSM selon des mécanismes conformes aux Critères Communs et FIPS 140-2/140-3, utilisant un DRBG (Générateur déterministe de bits aléatoires) approuvé. Ces méthodes assurent la production de clés cryptographiquement robustes, conformes aux exigences de sécurité du présent document.

4.4 Maintien en condition de conformité et d'actualité cryptographique

Le Prestataire :

- Assure un suivi régulier des recommandations de l'ENISA, du SOG-IS et des autorités européennes ;
- Met à jour les paramètres cryptographiques lorsque cela est nécessaire ;
- Garantit un niveau de robustesse minimal équivalent à 112 bits de sécurité (ou supérieur selon l'évolution des normes).

Toute évolution significative des algorithmes ou paramètres critiques est documentée dans la documentation technique associée et reflétée dans les mises à jour de la présente Déclaration de pratiques.

© Tous droits réservés be invest international SA - Toute reproduction ou diffusion même partielle interdite sans autorisation.